



PAN-OS: Remote Code Execution (RCE) in IKEv2 Processing

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-0263
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 18:16:14 UTC
Updated	2026-05-13 18:17:47 UTC
Description	A buffer overflow vulnerability in the IKEv2 processing of Palo Alto Networks PAN-OS® software allows an unauthenticated

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:Y/R:U/V:C/RE:H/U:R

Problem Types: CWE-787 | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:Y/R:U/V:C/RE:H/U:R

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Palo Alto Networks	Cloud NGFW	unaffected All custom
CNA	Palo Alto Networks	PAN-OS	affected 12.1.0 12.1.7, 12.1.4-h5 custom
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.12, 11.2.10-h6, 11.2.7-h13, 11.2.4-h17 custom
CNA	Palo Alto Networks	PAN-OS	affected 11.1.0 11.1.15, 11.1.13-h5, 11.1.10-h25, 11.1.7-h6, 11.1.6-h32, 11.1.4-h33 custom
CNA	Palo Alto Networks	PAN-OS	unaffected 10.2.0 custom
CNA	Palo Alto Networks	Prisma Access	unaffected All custom

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0263	psirt@paloaltonetworks.com	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: our internal security research teams (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-05-13T16:00:00.000Z	Initial publication.

Solutions

SOLUTIONS

CNA: VERSION MINOR VERSION SUGGESTED SOLUTION Cloud NGFW No action needed. PAN-OS 12.1 12.1.5 through 12.1.6 Upgrade to 12.1.7 or later. 12.1.2 through 12.1.4-h* Upgrade to 12.1.4-h5 or 12.1.7 or later. PAN-OS 11.2 11.2.11 or later Upgrade to 11.2.12 or later. 11.2.8 through 11.2.10-h* Upgrade to 11.2.10-h6 or 11.2.12 or later. 11.2.5 through 11.2.7-h* Upgrade to 11.2.7-h13 or 11.2.12 or later. 11.2.0 through 11.2.4-h* Upgrade to 11.2.4-h17 or 11.2.12 or later. PAN-OS 11.1 11.1.14 or later Upgrade to 11.1.15 or later. 11.1.11 through 11.1.13-h* Upgrade to 11.1.13-h5 or 11.1.15 or later. 11.1.8 through 11.1.10-h* Upgrade to 11.1.10-h25 or 11.1.15 or later. 11.1.7 through 11.1.7-h* Upgrade to 11.1.7-h6 or 11.1.15 or later. 11.1.5 through 11.1.6-h* Upgrade to 11.1.6-h32 or 11.1.15 or later. 11.1.0 through 11.1.4-h* Upgrade to 11.1.4-h33 or 11.1.15 or later. PAN-OS 10.2 No action needed. Prisma Access No action needed. All older unsupported PAN-OS versions Upgrade to a supported fixed version.

Workarounds

CNA: Customers using IKEv2 VPN can mitigate this issue by configuring IKEv2 VPN tunnels only with NIST approved Post Quantum Cryptography (PQC) ciphers.

Exploits

CNA: Palo Alto Networks is not aware of any malicious exploitation of this issue.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)